Claims

[108] 1. A method of authenticating a client to a communication system comprising the steps of:

receiving from a mobile station a subscriber identity corresponding to a subscriber of a mobile telecommunication network, wherein the mobile telecommunication network is separate from the communication system to which the client is to be authenticated;

sending the subscriber identity to an authentication block of the mobile telecommunication network;

receiving from the authentication block at least one challenge and at least one first secret based on a subscriber's secret specific to the subscriber identity;

sending the at least one challenge to the subscriber identity module;

receiving at least one second secret in response to the at least one challenge; and

using the second secret for authenticating the client.

[109] 2. The method of authenticating of claim 1 further comprising:

receiving a PIN from a user; and

transmitting wirelessly the PIN to the mobile station.

[110] 3. The method according to claim 2 further comprising:

encrypting the PIN before the step of transmitting.

[111] 4. The method according to claim 1 wherein the step of using further comprises:

encrypting the second secret to provide a encrypted second secret; and

transmitting the encrypted second secret to the communication system.

[112] 5. The method according to claim 4 wherein the step of using further comprises:

refreshing the encrypted second secret.

[113] 6. The method according to claim 1 wherein the step of sending the subscriber identity to an authentication block comprises sending wirelessly the subscriber identity to the authentication block; and the step of receiving from the authentication block comprises receiving wirelessly from the authentication block.

[114] 7. The method according to claim 1 wherein the steps of:

receiving from a mobile station a subscriber identity comprises receiving wirelessly from a mobile station a subscriber identity;

sending the at least one challenge comprises sending wirelessly the at least one challenge; and

receiving at least one second secret comprises receiving wirelessly at least one second secret.

[115] 8. The method of authenticating of claim 7 further comprising:

receiving a PIN from a user; and

transmitting wirelessly the PIN to the mobile station.

[116] 9. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting an infrared signal.

[117] 10. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting a radio signal.

[118] 11. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting a low power radio signal.

[119] 12. The method of authenticating of claim 8 wherein the step of transmitting wirelessly comprises transmitting an acoustic signal.

[120] 13. A client for authenticating a client to a communication system comprising:

a means for receiving from a mobile station a subscriber identity corresponding to a subscriber of a mobile telecommunication network, wherein the mobile telecommunication network is separate from the communication system to which the client is to be authenticated;

a means for sending the subscriber identity to an authentication block of the mobile telecommunication network;

a means for receiving from the authentication block at least one challenge and at least one first secret based on a subscriber's secret specific to the subscriber identity;

a means for sending the at least one challenge to the subscriber identity module;

a means for receiving at least one second secret in response to the at least one challenge; and

a means for using the second secret for authenticating the client.

[121] 14. The client for authenticating of claim 13 further comprising:

a means for receiving a PIN from a user; and

a means for transmitting wirelessly the PIN to the mobile station.

[122] 15. The client according to claim 14 further comprising:

a means for encrypting the PIN before the step of transmitting.

[123] 16. The client according to claim 13 wherein means for using further comprises:

a means for encrypting the second secret to provide a encrypted second secret; and

a means for transmitting the encrypted second secret to the communication system.

[124] 17. The method according to claim 16 wherein the step of using further comprises:

refreshing the encrypted second secret.

[125] 18. The client according to claim 13 wherein the a means for sending the subscriber identity to an authentication block comprises a means for sending wirelessly the subscriber identity to the authentication block; and the a means for receiving from the authentication block comprises a means for receiving wirelessly from the authentication block.

[126] 19. The client according to claim 13 wherein:

a means for receiving from a mobile station a subscriber identity comprises a means for receiving wirelessly from a mobile station a subscriber identity;

a means for sending the at least one challenge comprises a means for sending wirelessly the at least one challenge; and

a means for receiving at least one second secret comprises a means for receiving wirelessly at least one second secret.

[127] 20. The client of claim 19 further comprising:

a means for receiving a PIN from a user; and

a means for transmitting wirelessly the PIN to the mobile station.

[128] 21. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting an infrared signal.

[129] 22. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting a radio signal.

[130] 23. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting a low power radio signal.

[131] 24. The client of claim 19 wherein the a means for transmitting wirelessly comprises a means for transmitting an acoustic signal.

[132] 25. A method for providing at least one secret based on a subscriber identity comprising the steps of:

retrieving from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunication network;

sending wirelessly the subscriber identity to a client for authenticating the client to the communication system;

receiving wirelessly from the client at least one challenge based on a subscriber's secret specific to the subscriber identity;

generating at least one secret in response to the at least one challenge and

sending wirelessly the at least one secret.

[133] 26. The method of claim 25 wherein the method further comprises a step of wirelessly receiving a request.

[134] 27. The method of claim 26 wherein the request contains a PIN.

[135] 28. The method of claim 27 wherein the request contains an encrypted PIN.

[136] 29. The method of claim 27 further comprising a step of confirming that the PIN matches a identity module PIN.

[137] 30. A mobile station for providing at least one secret based on a subscriber identity comprising:

means for retrieving from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunication network;

means for sending wirelessly the subscriber identity to a client for authenticating the client to the communication system;

means for receiving wirelessly from the client at least one challenge based on a subscriber's secret specific to the subscriber identity;

means for generating at least one secret in response to the at

least one challenge and

means for sending wirelessly the at least one secret.

[138] 31. The mobile station of claim 30 wherein the method further comprises a means for wirelessly receiving a request.

[139] 32. The mobile station of claim 31 wherein the request contains a PIN.

[140] 33. The mobile station of claim 32 wherein the request contains an encrypted PIN.

[141] 34. The mobile station of claim 32 further comprising means for confirming that the PIN matches a identity module PIN.

[142] 35. A computer program product for controlling a client in order to authenticate the client to a communication system by using a subscriber identity module of a mobile telecommunications network, wherein the mobile telecommunications network is separate from the communications system to which the client is to be authenticated; the computer program product comprising:

computer executable program code to enable the client to retrieve from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunications network;

computer executable program code to enable the client to send the subscriber identity to an authentication block of the mobile telecommunications network;

computer executable program code to enable the client to receive from the authentication block at least one challenge and at least one first secret based on a subscriber's secret specific to the subscriber identity;

computer executable program code to enable the client to send the at least one challenge to the subscriber identity module;

computer executable program code to enable the client to receive at least one second secret in response to the at least one challenge; and

computer executable program code to enable the client to use the second secret for authenticating the client; characterised in that the subscriber identity module is accessed over a local wireless link when retrieving the subscriber identity.

[143] 36. A computer program product for controlling a client in order to authenticate the client to a communication system by using a subscriber identity module of a mobile telecommunications network, wherein the mobile telecommunications network is separate from the communications system to which the client is to be authenticated; the computer program product comprising:

computer executable program code to enable the client to retrieve from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunications network;

computer executable program code to enable the client to send the subscriber identity to an authentication block of the mobile telecommunications network;

computer executable program code to enable the client to receive from the authentication block at least one challenge and at least one first secret based on a subscriber's secret specific to the subscriber identity;

computer executable program code to enable the client to send the at least one challenge to the subscriber identity module;

computer executable program code to enable the client to receive at least one second secret in response to the at least one challenge; and

computer executable program code to enable the client to use the second secret for authenticating the client; characterised in that the subscriber identity module is accessed over a local wireless link when retrieving the subscriber identity.

[144] 37. A computer program product for controlling a device for authentication a client to a communications system using a subscriber identity module of a mobile telecommunications network, wherein the communications system is separate from the mobile telecommunications network, the computer program product comprising:

computer executable program code to enable the device to retrieve from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunications network;

computer executable program code to enable the device to send the subscriber identity to a client over a local wireless link for authenticating the client to the communications system;

computer executable program code to enable the device to receive over the local wireless link from the client at least one challenge based on a subscriber's secret specific to the subscriber identity;

computer executable program code to enable the device to provide the at least one challenge to the subscriber identity module and receiving at least one authentication secret in response to the challenge; and

computer executable program code to enable the device to send the at least one authentication secret over the local wireless link to the client.